STATE OF SOUTH CAROLINA CYBERSECURITY PLAN

October 2023

Approved by SC Cybersecurity Planning and Advisory Committee on 10/03/2023
Revised by committee on 05/20/2025

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

INTRODUCTION

The South Carolina Comprehensive Cybersecurity Plan (CCP) plays a pivotal role in guiding the state's efforts to establish and enhance cyber resilience. It encapsulates all five essential aspects of the National Institute of Standards and Technology (NIST) Cybersecurity Framework v1.1: identification, protection, detection, response, and recovery. South Carolina has integrated existing plans, structures, and other relevant initiatives to form our inclusive cybersecurity strategy. Leveraging pre-existing structures and capabilities empowers South Carolina to establish governance and a framework to efficiently address significant cybersecurity demands while optimally utilizing available resources. By incorporating feedback from local jurisdictions, the State of South Carolina fulfills requirement e.2.A.ii. of the State and Local Cybersecurity Grant Program (SLCGP).

The CCP is a three-year strategic planning document that contains the following components:

- Vision and Mission: Articulates the vision and mission for improving cybersecurity resilience interoperability over the next three years.
- Cybersecurity Plan Elements: Maps the technology and operations to the Cybersecurity Capabilities Assessment (Appendix A), an analysis of South Carolina's cybersecurity maturity against the 16 required cybersecurity elements. The Plan was built using the results of the Assessment and goals prioritized with the goal of rapidly maturing South Carolina's cybersecurity capabilities.
- Funding: Describes the strategy for allocating funds received from the SLCGP and matching funds provided by the state of South Carolina from existing projects along with in-kind hours donated by the organizations supporting the effort.
- Assessment of Capabilities and Needs: Describes how inputs from local governments were used to reduce overall cybersecurity risk across the eligible entity and ensure that the developed plan takes a holistic view.
- Implementation Plan: Describes the State of South Carolina's plan to implement, maintain, and update the Cybersecurity Plan to enable continued evolution of and progress toward the identified goals. The implementation plan will include the resources and timeline where practicable.
- Organization, Roles, and Responsibilities: Describes the leaders and organizations responsible for executing the tasks and activities to achieve the goals and support the mission and vision. The leaders and organizations collaborate with local entities; however, the Plan is a guiding document and does not create any authority or direction over local entities.
- Metrics & Milestones: Describes how South Carolina will measure the outputs and outcomes of the program across the entity.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework[1], included in Figure 1, helps guide key decisions made about risk management activities through various levels

[1] https://www.nist.gov/cyberframework/getting-started

of organizations from senior executives to business and process level personnel, including implementation and operations.

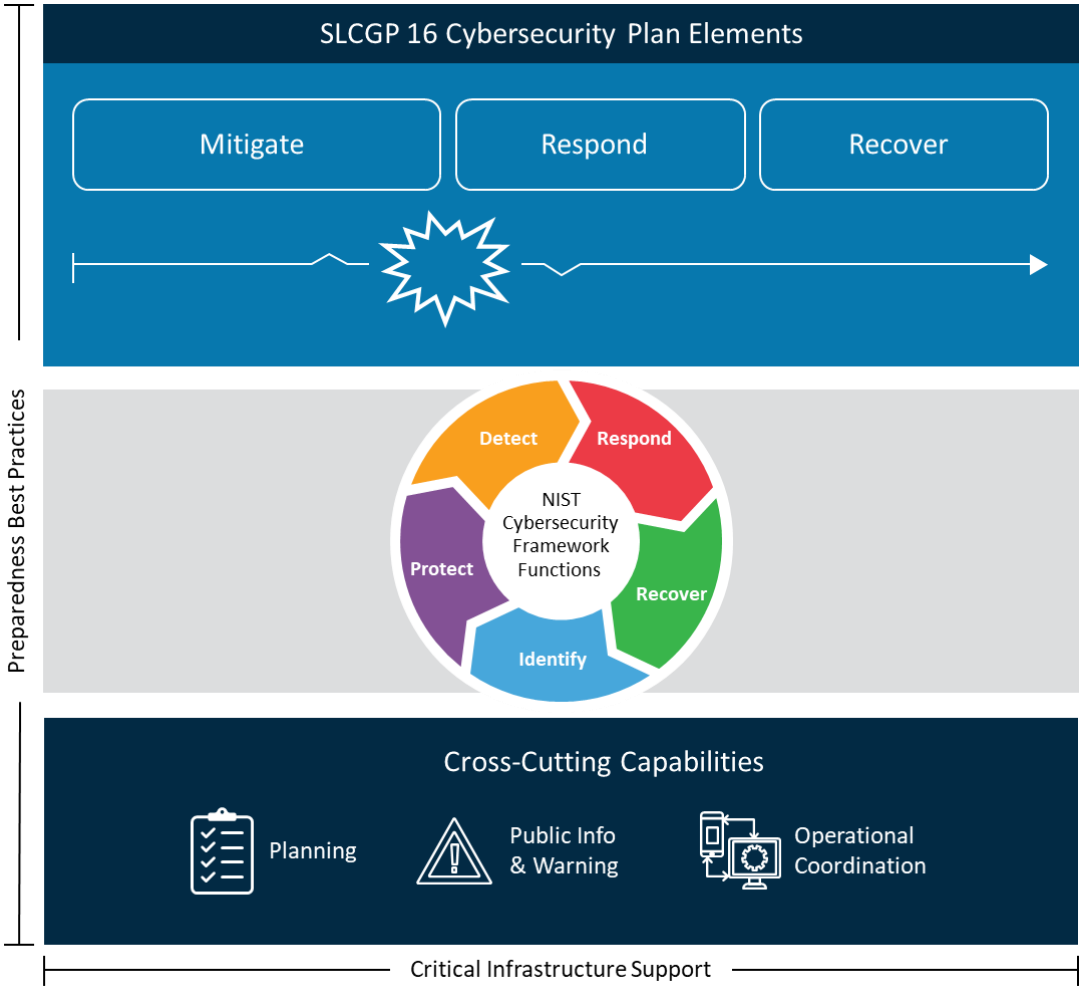

Figure 1: Achieving Cyber Resilience Through Comprehensive Cybersecurity Plans

Vision and Mission

This section describes South Carolina's vision and mission for improving cybersecurity:

Vision:

A state where all South Carolinians are protected from cyber threats, through a collaborative effort between state, local, and critical infrastructure entities that continuously expand and advance cybersecurity training, practices, and adoption of cybersecurity technology.

Mission:

To increase cyber resiliency in South Carolina by leveraging committees, partnerships, and working groups to mature cybersecurity practices and incident response across the state.

Cybersecurity Plan Overview

The Plan's principal purpose is to increase the cyber resiliency of South Carolina's state and local government entities. After reviewing incident response data, cyber posture reviews, and conducting interviews, the SLCGP committee identified goals that would have the biggest impact on improving the cybersecurity practices of these entities. From these goals, objectives were identified that support achieving each goal to aid in meeting and accomplishing the Plan's principal purpose.

As the Plan unfolds under the guidance of the SLCGP committee, the focus will be on specified milestones and strategies, driving the necessary tasks that will ensure the Plan's realization. Nested within these strategies and tasks are the goals and 16 required elements prescribed by the Cybersecurity and Infrastructure Security Agency (CISA). For a clearer correlation between the mandated goals and required elements with this Plan's goals, strategies, and tasks, refer to Appendix A.

At least annually, the Committee will engage in a progress assessment and fine-tuning of the Plan. This proactive approach ensures continuous alignment with the Plan's ambitions, strategies, and tasks, especially when navigating an ever-evolving landscape of cyber challenges.

Cybersecurity goals and objectives include the following:

Cybersecurity Program	
Program Goal	**Program Objectives**
1. Enhancing Cyber Resilience	1.1 Facilitate Endpoint Detection and Response (EDR) adoption to raise visibility across network infrastructure and protect state and local government assets in real-time.
	1.2 Conduct and participate in interactive cyber tabletop exercises to assess and improve organization readiness.
	1.3 Support new and existing vulnerability scanning capabilities.
	1.4 Promote and adopt the use of .gov top-level domains to increase confidence in the legitimacy of state and local government websites and communications.
	1.5 Develop and participate in a statewide comprehensive Managed Detection and Response (MDR) function capable of monitoring, alerting, and responding to cybersecurity incidents.
	1.6 Promote the adoption of Domain Name Service (DNS), email, and web filtering.
	1.7 Promote the adoption of multi-factor authentication.
	1.8 Deploy a Security Information and Event Management (SIEM) service to ingest security logs, improving threat visibility and reducing the time to detect and respond to incidents.
	1.9 Leverage cloud-based security solutions to support continuous monitoring, flexibility, scalability, and more direct access to provider expertise as well as robust security features such as identity and access management, data classification, or data loss prevention.
	1.10 Deploy immutable storage solutions that protect against unauthorized tampering or deletion of backup data.
2. Cyber Training and Workforce Development (Aligned with NICE Workforce Framework for Cybersecurity)	2.1 Deliver and participate in live fire cyber training through a shared platform to increase incident response readiness statewide.
	2.2 Support and participate in cyber training to ensure on-demand incident response capabilities and essential skills are current.
	2.3 Support new and existing Phishing and Security Awareness capabilities across state and local government entities.
	2.4 Participate in initiatives aimed at fostering cybersecurity training and educational programs to enhance the professional growth and retraining of existing personnel.
	2.5 Grow and support cybersecurity internship, apprenticeship, and scholarship for service programs necessary to develop a proficient cyber workforce.
3. Risk Management	3.1 Support, promote, and utilize CISA's Cross-sector Performance Goals (CPGs).
	3.2 Support, promote, and utilize CISA's Known Exploited Vulnerabilities Catalog in prioritizing patching decisions.
	3.3 Develop and produce cybersecurity progress reports to key stakeholders that identify trends, risks, and emerging threats.

Program Goal	Program Objectives
	3.4 Compile and provide basic cybersecurity policy templates for organizations to customize and implement.
4. Strengthening Information Sharing	4.1 Enhance collaboration and communication with stakeholders.
	4.2 Conduct thorough post-incident reviews after each cybersecurity incident to communicate areas for improvement and implement changes based on lessons learned.
	4.3 Develop and distribute relevant security awareness materials, alerts, and advisories.
	4.4 Foster improved collaboration between statewide cybersecurity initiatives and operators of critical infrastructure and vital resources in South Carolina.

Each goal and its associated objectives have a timeline with a target completion date, and one or more owners that will be responsible for overseeing and coordinating its completion. Accomplishing goals and objectives will require support and cooperation from the individuals, groups, or agencies listed above, and may be added as formal agenda items for review during regular governance body meetings.

FUNDING & SERVICES

The Plan was formulated with the acknowledgment that the SLCGP will provide supplemental backing to enhance the resources of state and local government entities. This aims to foster sustainability beyond the designated performance periods. The state has assessed the necessary funding for the future and taken steps to ensure that the projects will continue to be supported through their completion.

Resource Allocation & Prioritization

Efficiently prioritizing and promptly allocating resources is crucial in optimizing the impact of the funds granted by the SLCGP to the State. When deliberating on the most effective distribution of funds, services, equipment, and software to state and local government entities, the Committee will weigh various factors which encompass, but are not confined to these considerations:

- Endeavors that mitigate cybersecurity vulnerabilities affecting public health, citizen welfare, safety, the economy, or state or national security.
- Undertakings that directly help safeguard the cybersecurity of essential infrastructure systems for state or local government entities.
- Initiatives that align with the program goals and the 16 key elements outlined in the Statewide Cyber Plan.

In addition, the Committee will ensure at least 80% of the funds, services, equipment, and software are allotted to local government entities with 25% of that 80% allotted to rural areas.

ASSESSING CAPABILITIES AND NEEDS

The state and local government capabilities that exist in the state of South Carolina have been assessed using data collected through the SC CIC program to include incident response engagements, cyber posture reviews, and interviews with these entities.

- Incident response – While responding to cybersecurity incidents that affect critical infrastructure in the State, SC CIC performs lessons learned at the end of each engagement to identify security weaknesses in the affected entities. From that data, trends can be identified that indicate where efforts should be focused to improve cybersecurity for the State.
- Cyber Posture Reviews (CPRs) – The Cyber Posture Review is a self-assessment that SC CIC delivers to participants which aligns with CISA's Cybersecurity Performance Goals (CPGs). The CPR data provides unique insights from a strategic perspective across multiple entities. As state and local government falls under the 16 critical infrastructure sectors, this compiled data can be used to identify gaps that can be addressed to strengthen the cybersecurity of those entities.
- Interviews – SC CIC maintains two-way communication with hundreds of entities in the State, which includes state and local governments. These existing relationships allow for direct interactions with local government IT and security staff, which were leveraged to get feedback on issues that can be addressed by the projects in the SLCGP.

The SLCGP committee leveraged these data-driven insights to identify goals that would have the biggest impact on improving the State's overall cybersecurity posture while aligning with the 16 critical objectives identified by CISA.

IMPLEMENTATION PLAN

Organization, Roles, and Responsibilities

The SLCGP Planning Committee Charter outlines the roles, responsibilities, and duties of the SLCGP Planning Committee (the "Committee") in creating, overseeing, evaluating, and modifying this Plan, as needed. Concurrently, it prioritizes funding efforts and greenlights projects aimed at diminishing cyber risks throughout South Carolina's state and local government entities, in alignment with the Infrastructure Investment and Jobs Act (IIJA) and the SLCGP Notice of Funding Opportunity (NOFO). The SLCGP Committee is currently composed of representation from multiple entities that include:

- South Carolina Governor's Office
- South Carolina Law Enforcement Division (SLED)
    - *South Carolina Critical Infrastructure Cybersecurity (SC CIC)*
- South Carolina Department of Administration
    - *Office of Technology and Information Security (OTIS)*
- South Carolina Office of the Adjutant General
    - *National Guard and Emergency Management*

- South Carolina Election Commission
- Various local government entities

This Plan promotes a comprehensive state defense approach but simultaneously acknowledges the authority, roles, and duties of individual state and local government entities in South Carolina. Each body holds primary responsibility and accountability for upholding its distinct cybersecurity program and performing the daily security and IT management functions of its designated systems and networks. Every state and local government agency is tasked with defining its risk tolerance while instituting administrative, physical, and technical protocols and safeguards based on those limits. Resources like funds, services, hardware, and software, potentially sourced from the SLCGP, are not intended to override, or replace their existing powers or duties. Rather, they aim to boost the agencies' resources, elevating their security stances and bolstering their resilience against evolving threats.

METRICS

Throughout the course of the SLCGP grant process, the Planning Committee will consistently assess advancements made in accordance with the established goals, objectives, and action items outlined in this plan. The Planning Committee and the SAA will collaboratively formulate and support collection of administrative, financial, and other pertinent grant management metrics throughout the duration of the grant. It remains the duty of the Planning Committee to monitor progress through meaningful metrics and comprehensive reporting. A brief description of the metrics that will be used for tracking progress can be found in Appendix C.

APPENDIX A: CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

COMPLETED BY THE COMMITTEE				FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of State Local Tribal and Territorial (SLTT) within the Eligible Entity**	**Select capability level from:** Foundational Fundamental Intermediary Advanced	**Project # (s)** *(If applicable – as provided in Appendix B)*	**Met**
1. Manage, monitor, and track information systems, applications, and user accounts.	The South Carolina Department of Information Security (DIS) provides security monitoring services for state agencies that address basic security use cases. The Comprehensive Cybersecurity Plan (CCP) committee has identified a gap in comparable monitoring with local government entities.	Foundational	SCSLCGP-02, SCSLCGP-05, SCSLCGP-07, SCSLCGP-08, SCSLCGP-12	
2. Monitor, audit, and track network traffic and activity.	The DIS provides security monitoring services for state agencies that address basic security uses cases. SC's local government entities have basic network monitoring capabilities that can be improved.	Fundamental	SCSLCGP-02, SCSLCGP-07, SCSLCGP-08, SCSLCGP-11	
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts.	The DIS provides a security framework to help prepare state agencies for an adverse cyber event and provide response assistance. The South Carolina Critical Infrastructure Cybersecurity (SC CIC) program similarly assists local government entities, but capabilities must be expanded to support the need.	Foundational	SCSLCGP-01, SCSLCGP-02, SCSLCGP-03, SCSLCGP-04, SCSLCGP-05, SCSLCGP-06, SCSLCGP-07, SCSLCGP-08, SCSLCGP-10, SCSLCGP-11, SCSLCGP-12	
4. Implement a process of continuous cybersecurity vulnerability	The DIS provides resources to state agencies to aid in the practice of identifying and mitigation risk. SC CIC	Fundamental	SCSLCGP-04, SCSLCGP-05,	

assessment and threat mitigation, prioritized by degree of risk.	assists and provides resources to local government entities but must be expanded to support the need.		SCSLCGP-07, SCSLCGP-08	
5. Adopt and use best practices and methodologies to enhance cybersecurity in alignment with NIST.	This is a continuous effort from contributing entities to adopt and follow the list of best practices outlined below: - Implement multi-factor authentication - Implement enhanced logging - Data encryption for data at rest and in transit - End use of unsupported/end of life software and hardware that are accessible from the internet - Prohibit use of known/fixed/default passwords and credentials - Ensure the ability to reconstitute systems (backups) - Migration to the .gov internet domain	Foundational	SCSLCGP-02, SCSLCGP-04, SCSLCGP-05, SCSLCGP-06, SCSLCGP-12	
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain.	All state agencies are required to use the sc.gov domain per policy unless a specific exception is given to use the .gov domain. Local government entity adoption of the .gov domain is ongoing.	Fundamental	SCSLCGP-04, SCSLCGP-06	
7. Ensure continuity of operations, including by conducting exercises.	Some state agencies and local government entities conduct cybersecurity exercises such as tabletops, but a wider adoption of exercises is needed.	Fundamental	SCSLCGP-01, SCSLCGP-03, SCSLCGP-06, SCSLCGP-09	
8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel in alignment with the NICE Workforce Framework for Cybersecurity.	This is an ongoing effort of several cybersecurity working groups and state entities to address cybersecurity workforce challenges.	Fundamental	SCSLCGP-01, SCSLCGP-03, SCSLCGP-06, SCSLCGP-09	
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks.	Most state agencies have disaster recovery and business continuity (DR/BC) plans to ensure continuity of data networks; however, the maturity and the ability to execute these plans varies greatly. Many local government entities lack any DR/BC plans.	Fundamental	SCSLCGP-10	
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and	This varies across entities. Some are more advanced, while others are still developing. Overall, while progress	Fundamental	SCSLCGP-01, SCSLCGP-02,	

cybersecurity threats relating to critical infrastructure and key resources.	has been made, there's a need for consistent effort to mature this capability across all entities.		SCSLCGP-03, SCSLCGP-04, SCSLCGP-05, SCSLCGP-06, SCSLCGP-07, SCSLCGP-08, SCSLCGP-10, SCSLCGP-11	
11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.	SC CIC facilitates bilateral intelligence on cyber events, threats, and indicators of compromise between federal partners and the local government entities that participate in the SC CIC program.	Fundamental	SCSLCGP-04, SCSLCGP-07, SCSLCGP-08, SCSLCGP-09	
12. Leverage cybersecurity services offered by the Department of Homeland Security.	SC CIC currently advertises and promotes services provided by the Department of Homeland Security and will communicate the requirement of SLCGP funding recipients and subrecipients to complete the NCSR annually and utilize CISA's cyber hygiene services that include Web Application and Vulnerability Scanning.	Fundamental	SCSLCGP-04, SCSLCGP-06	
13. Implement an Information Technology (IT) and Operational Technology (OT) modernization cybersecurity review process that ensures alignment between IT and OT cybersecurity objectives.	The IT and OT modernization cybersecurity review process is currently being developed for local government entities. Further development and refinement are needed as well as expansion to State entities.	Fundamental	SCSLCGP-01, SCSLCGP-03, SCSLCGP-04, SCSLCGP-10	
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats while coordinating with local governments and associations.	SC CIC works with over 250 critical infrastructure entities in the state which includes local and rural government as well as their associations. The cybersecurity risk and threat strategies coordinated with these existing agencies will continue to be developed and extended to new participants as the SLCGP is carried out.	Fundamental	SCSLCGP-01, SCSLCGP-03, SCSLCGP-04, SCSLCGP-05, SCSLCGP-06, SCSLCGP-07, SCSLCGP-09	
15. Ensure rural areas have adequate access to, and participation in, plan activities.	SC CIC continuously works with rural local government entities to provide services and access to resources to develop cyber capabilities.	Fundamental	All	
16. Distribute funds, items, services, capabilities, or activities to local governments.	SC CIC delivers security services to local governments as part of the program's founding mission. These services will be enhanced and expanded in alignment with the CCP.	Fundamental	All	

APPENDIX B: PROJECT SUMMARY WORKSHEET

Purpose: The **Project Summary Worksheet** is a list of cybersecurity projects that the entity plans to complete to develop or improve any needed cybersecurity capabilities identified in **Appendix A: Cybersecurity Plan Capabilities Assessment**.

1.	2. Project Name	3. Project Description	4. Related Required Element #	5. Objective Alignment	6. Cost	7. Status	8. Priority	9. Project Type
SCSLCGP-01	Cyber range	Build a cloud-hosted cyber range to facilitate both live fire exercises and individual cyber defense upskilling that is accessible from everywhere in the state.	3, 7, 8, 13, 16	1.1, 1.5, 2.4	$250,000	Future	High	Train Exercise
SCSLCGP-02	Endpoint protection solution	Procure and implement an EDR solution at eligible state and local government entities.	1, 2, 3, 5, 15, 16	2.1, 2.2	$1,600,000	Future	High	Equip
SCSLCGP-03	Cybersecurity workforce development	Create, establish, and offer a range of cybersecurity training options, both online and in-person.	7, 8	2.4, 2.5	$367,529	Future	Medium	Plan Organize Train
SCSLCGP-04	CPR expansion	Continue support of the existing Cyber Posture Review (CPR) and expand it to include more organizations in the state.	3, 4, 6, 9, 10, 13, 14, 15, 16	3.1, 3.2, 4.4	$50,000	Ongoing	Medium	Plan Organize
SCSLCGP-05	Vulnerability scanning service expansion	Expand SC CIC's current external vulnerability scanning service that is provided to critical infrastructure organizations to include internal scanning options.	1, 3, 4, 10, 15, 16	1.3, 3.3, 3,4	$350,000	Ongoing	Medium	Equip
SCSLCGP-06	Security awareness campaign	Create and distribute security awareness material that educates state and local government of no-cost government provided security services and	5, 6, 7, 12, 14, 15, 16	1.4, 2.3, 2.4, 4.4	$25,000	Future	Low	Plan Organize Train

		increase adoption rate of .gov domains.						
SCSLCGP-07	SC threat intelligence program expansion	Provide SC CIC's South Carolina-tailored threat intelligence services to more state and local government entities.	1, 2, 3	4.3, 2.3	$100,000	Ongoing	High	Plan Organize Train
SCSLCGP-08	Dark web cyber security monitoring service expansion	Expand dark web security monitoring services for the domains of agencies that are participating in the SC CIC program to more government organizations in the state.	1, 2, 3, 4	4.3, 2.3	Funding currently	Ongoing	High	Plan Organize Train
SCSLCGP-09	SC cybersecurity conference	Host a cybersecurity conference for state and local government entities to attend, network, and collaborate with the state's cybersecurity professionals.	5, 6, 7, 12, 14, 15, 16	1.4, 2.3, 2.4, 4.4	$100,000	Future	Low	Plan Organize Train
SCSLCGP-10	Cybersecurity policy templates	Compile and provide basic cybersecurity policy templates for organizations to customize and implement.	3, 7, 9, 13, 14, 15, 16	3.5	$35,000	Future	Medium	Plan Equip
SCSLCGP-11	DNS Filtering	Provide state and local government entities with the ability to filter DNS by content categories.	1	1.6	$100,000	Future	Low	Plan Equip
SCSLCGP-12	Multi-factor authentication	Implementing multi-factor authentication	1	1.7	$400,000	Future	Medium	Plan Equip Organize Train
SCSLCGP-M&A	SAA Management and Administration	Required funds for grant Administration.	1, 2, 3, 4	All	$183,028	Future	Low	Plan
SCSLCGP-CISA Previously Approved	Plan Development	Write the statewide cybersecurity plan for South Carolina.	1, 2, 3, 4	All	$100,000	Current	Medium	Plan

APPENDIX C: METRICS

The below table should reflect the goals and objectives the Cybersecurity Planning Committee establishes.

Cybersecurity Plan Metrics			
Program Goal	**Program Objectives**	**Metrics**	**Metrics Description**
1. Enhancing Cyber Resilience	1.1	Number of entities onboarded with EDR.	Reported by sub recipient. Reporting frequency: Annually.
	1.2	Number of tabletop exercises hosted. Number of organizations trained.	Reported by sub recipient. Reporting frequency: Annually.
	1.3	Number of organizations conducting scans.	Reported by sub recipient. Reporting frequency: Annually.
	1.4	Number of organizations that adopted the use of .gov top-level domains.	Reported by sub recipient. Reporting frequency: Annually.
	1.5	Number of organizations participating in MDR	Reported by sub recipient. Reporting frequency: Annually.
	1.6	Number of organizations that adopted DNS filtering	Reported by sub recipient. Reporting frequency: Annually.
	1.7	Number of organizations utilizing multi-factor authentication.	Reported by sub recipient. Reporting frequency: Annually.
2. Cyber Training and Workforce Development	2.1	Number of users utilizing live fire cyber training.	Reported by sub recipient. Reporting frequency: Annually.
	2.2	Number of organizations participating in cybersecurity training.	Reported by sub recipient. Reporting frequency: Annually.
	2.3	Number of organizations that adopted phishing and security awareness capabilities.	Reported by sub recipient. Reporting frequency: Annually.
	2.4	List of initiatives participated in.	Reported by sub recipient. Reporting frequency: Annually.
	2.5	Number of internships facilitated.	Reported by sub recipient. Reporting frequency: Annually.
3. Risk Management	3.2	Number of organizations that have received education about KEV.	Reported by sub recipient. Reporting frequency: Annually.
	3.3	Number of progress reports created.	Reported by sub recipient. Reporting frequency: Annually.
	3.4	Number of policy templates created.	Reported by sub recipient.

Program Goal	Program Objectives	Metrics	Metrics Description
		Number of organizations provided with templates.	Reporting frequency: Annually.
4. Strengthen Information Sharing and Collaboration	4.1	Number of information sharing documents distributed to stakeholders.	Reported by sub recipient. Reporting frequency: Annually.
	4.2	Number of post-incident reviews conducted.	Reported by sub recipient. Reporting frequency: Annually.
	4.3	Number of security awareness campaigns conducted.	Reported by sub recipient. Reporting frequency: Annually.
	4.4	List of initiatives supported.	Reported by sub recipient. Reporting frequency: Annually.